
Micro Focus Fortify Security Assistant Plugin for Eclipse

Software Version: 18.20

User Guide

Document Release Date: November 2018
Software Release Date: November 2018



Legal Notices

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

<https://www.microfocus.com>

Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors ("Micro Focus") are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Except as specifically indicated otherwise, a valid license from Micro Focus is required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

© Copyright 2015 - 2018 Micro Focus or one of its affiliates

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

<https://www.microfocus.com/support-and-services/documentation>

Contents

Preface	4
Contacting Micro Focus Fortify Customer Support	4
For More Information	4
About the Documentation Set	4
Change Log	5
Chapter 1: Installation and Configuration	6
Fortify Security Assistant Plugin for Eclipse	6
Installing Fortify Security Assistant for Eclipse	6
Uninstalling Fortify Security Assistant for Eclipse	7
Configuring Fortify Security Assistant for Eclipse	8
Updating Security Content	10
Chapter 2: Using Fortify Security Assistant for Eclipse	11
Finding Security Issues as you Write Java Code	11
Working with Issues in the Code	12
Scanning Projects for Issues	13
Working with the Security Assistant Issues View	13
Showing Suppressed Issues	15
Unsuppressing Issues	15
Hiding Security Issues	15
Revealing Previously Hidden Security Issues	16
Send Documentation Feedback	17

Preface

Contacting Micro Focus Fortify Customer Support

If you have questions or comments about using this product, contact Micro Focus Fortify Customer Support using one of the following options.

To Manage Your Support Cases, Acquire Licenses, and Manage Your Account

<https://softwaresupport.softwaregrp.com>

To Call Support

1.844.260.7219

For More Information

For more information about Fortify software products:

<https://software.microfocus.com/solutions/application-security>

About the Documentation Set

The Fortify Software documentation set contains installation, user, and deployment guides for all Fortify Software products and components. In addition, you will find technical notes and release notes that describe new features, known issues, and last-minute updates. You can access the latest versions of these documents from the following Micro Focus Product Documentation website:

<https://www.microfocus.com/support-and-services/documentation>

Change Log

The following table lists changes made to this document. Revisions to this document are published between software releases only if the changes made affect product functionality.

Software Release / Document Version	Changes
18.20	Updated: <ul style="list-style-type: none">• "Configuring Fortify Security Assistant for Eclipse" on page 8 - You can now import Fortify Software Security Content from a local ZIP file
18.10	Updated: <ul style="list-style-type: none">• Minor edits to incorporate branding changes• "Configuring Fortify Security Assistant for Eclipse" on page 8 - How to import Fortify Software Security Content locally
17.20	Updated: Release date and version number

Chapter 1: Installation and Configuration

This section contains the following topics:

- [Fortify Security Assistant Plugin for Eclipse](#) 6
- [Installing Fortify Security Assistant for Eclipse](#) 6
- [Uninstalling Fortify Security Assistant for Eclipse](#) 7
- [Configuring Fortify Security Assistant for Eclipse](#) 8
- [Updating Security Content](#)10

Fortify Security Assistant Plugin for Eclipse

The Fortify Security Assistant for Eclipse integrates with the Eclipse Java development environment. Fortify Security Assistant for Eclipse works with a portion of the Fortify security content to provide alerts to potential security issues as you write your Java code. Fortify Security Assistant for Eclipse provides detailed information about security risks and recommendations for how to secure the potential issue. Fortify Security Assistant for Eclipse can detect:

- Potentially dangerous uses of functions and APIs
- Issues caused by tainted data reaching vulnerable functions and APIs at the intra-class level

Fortify Security Assistant for Eclipse requires :

- A valid Fortify license to scan for issues
- Up-to-date Fortify Software Security Content

You are prompted to provide a license file and Fortify Software Security Content if necessary. For information about how to obtain a Fortify license file, see the *Micro Focus Fortify Software System Requirements* document.

Installing Fortify Security Assistant for Eclipse

You can install the Fortify Security Assistant Plugin for Eclipse on Windows, Linux, and macOS operating systems. To update from an earlier version of Fortify Security Assistant Plugin for Eclipse, you must first remove the existing version. For information about how to uninstall the plugin, see "[Uninstalling Fortify Security Assistant for Eclipse](#)" on the next page.

Note: These instructions describe a third-party product and might not match the specific, supported version you are using. See your product documentation for the instructions for your version.

To install Fortify Security Assistant for Eclipse:

1. Start Eclipse.
2. Select **Help > Install New Software**.
The Install wizard starts and displays the **Available Software** step.
3. Click **Add**.
4. Click **Archive**, and then locate and select `Fortify_SecurityAssistant_Eclipse_Plugin_<version>.zip`.
5. Click **Add**.
6. Select the **Fortify Security Assistant Plugin** check box, and then click **Next**.
The **Install Details** step lists **Fortify Security Assistant Plugin For Eclipse**.
To view version and copyright information about the plugin in the **Details** area, click the plugin name.
7. Click **Next**.
8. On the **Review Licenses** step, review and accept the license agreement.
9. Click **Finish**.
10. To complete the installation and restart Eclipse, click **Restart Now** when prompted.

The menu bar now includes the **Fortify** menu.

You might be prompted to specify a Fortify license. Click **Browse** in the Locate Fortify License File dialog box, navigate to the license file, and then click **OK**. Fortify Security Assistant for Eclipse verifies the license file and then attempts to download the Fortify Software Security Content from the Fortify Customer Portal. To import Fortify Software Security Content from a local archive, see "[Configuring Fortify Security Assistant for Eclipse](#)" on the next page.

Uninstalling Fortify Security Assistant for Eclipse

Note: These instructions describe a third-party product and might not match the specific, supported version you are using. See your product documentation for the instructions for your version.

To uninstall Fortify Security Assistant Plugin for Eclipse:

1. Start Eclipse.
2. Select **Help > About Eclipse IDE**, and then click **Installation Details**.
3. On the **Installed Software** tab, select **Fortify Security Assistant Plugin for Eclipse**.
4. Click **Uninstall**.
5. In the Uninstall window, click **Finish**.
6. To implement the change and restart Eclipse, click **Yes** when prompted.


Configuring Fortify Security Assistant for Eclipse

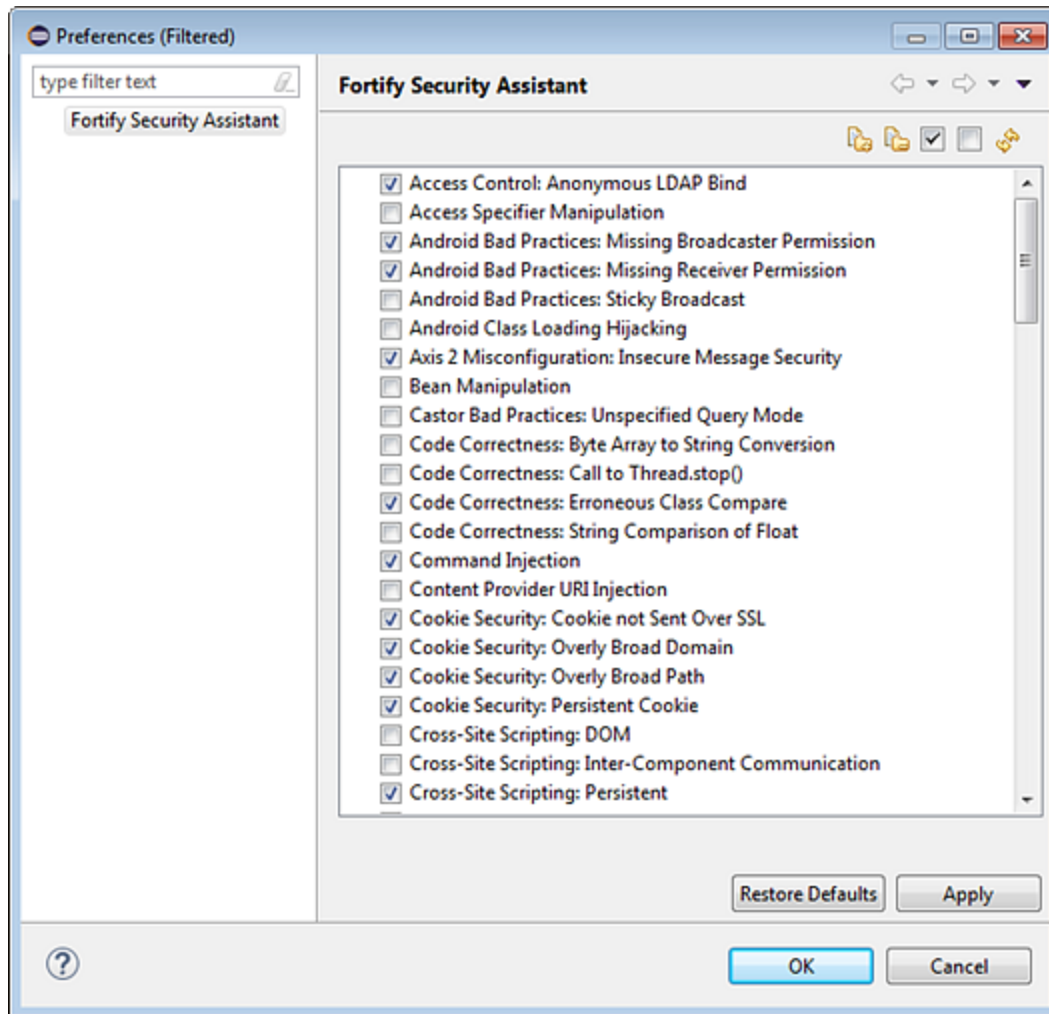
Fortify Security Assistant for Eclipse requires Fortify Software Security Content to detect issues. You can specify the categories of issues you want Fortify Security Assistant for Eclipse to detect. You can specify these settings for the workspace or for a particular project.

To configure settings for the workspace or for a project:


1. Do one of the following:
 - To configure settings for the workspace, select **Fortify > Configure Security Assistant**.
 - To configure settings for a project:
 - i. Right-click a project, and then select **Properties**.
 - ii. In the left panel, select **Fortify Security Assistant**.
 - iii. Select **Enable project specific settings**.


Note: You can also specify the category of issues from a Fortify Security Assistant for Eclipse tooltip in the Code editor. Click **Configure Security Assistant** , and then click **Configure Workspace** or **Configure Project**.

2. If Fortify Software Security Content has not been loaded, click **Load Security Content**.
Fortify Security Assistant for Eclipse first attempts to load the Fortify Software Security Content from a default installation of Micro Focus Fortify Static Code Analyzer. Otherwise, Fortify Security Assistant for Eclipse attempts to download the Fortify Software Security Content from the Fortify Customer Portal.
If you do not have a network connection to the Fortify Customer Portal, you can import local rules by clicking **Import Security Content** . You can import ZIP, XML, or BIN files.



3. Select the categories of issues you want to detect.
You can right-click in the list of categories, and then select **Select All** or select **Clear All (but one)**.

4. To import custom rules:
 - a. Click **Import Security Content** .
 - b. Navigate to where your custom file is located, select the XML, and then click **Open**.

Note: To remove any rules you previously imported custom rules, click **Clear All Imported Security Content** . You cannot undo this action.

5. Click **Apply**.
6. Click **OK**.

Fortify Security Assistant Plugin for Eclipse re-inspects the project to refresh any issues reported so that it matches your configuration settings.

Updating Security Content

To optimize Fortify Security Assistant for Eclipse functionality, you must have complete and up-to-date Fortify Software Security Content. To update security content from the Fortify Customer Portal, you must be connected to the Internet and have your Eclipse network connections configured to access the Fortify Customer Portal (<https://update.fortify.com>).

Note: To update Fortify Software Security Content from a local file, import it as described in step 2 in "[Configuring Fortify Security Assistant for Eclipse](#)" on page 8.

To obtain the latest security content from the Fortify Customer Portal:

- Select **Fortify > Update Security Content**.

Chapter 2: Using Fortify Security Assistant for Eclipse

Fortify Security Assistant for Eclipse notifies you of any detected issues as you write your code. You can also have Fortify Security Assistant for Eclipse examine an entire project and then review possible security issues (see "Scanning Projects for Issues" on page 13).

This section contains the following topics:

Finding Security Issues as you Write Java Code	11
Working with Issues in the Code	12
Scanning Projects for Issues	13
Working with the Security Assistant Issues View	13
Hiding Security Issues	15
Revealing Previously Hidden Security Issues	16

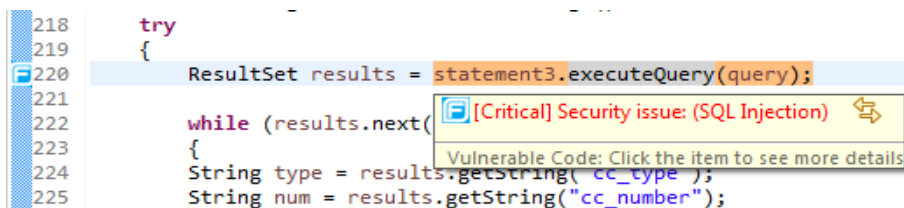
Finding Security Issues as you Write Java Code

You can review the information about the security issues and update the code as appropriate.

To review the security issues:

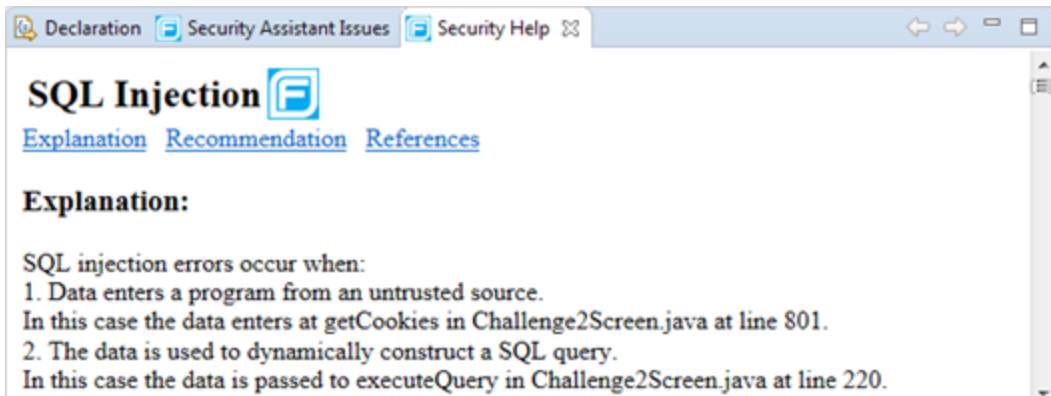
- Fortify Security Assistant for Eclipse highlights possible security issues in the code. It also tags the issue with an icon in the left border of the editor area. Pause your cursor over the highlighted code to open a tooltip that briefly describes the issue as shown in the following example:


```
218     try
219     {
220         ResultSet results = statement3.executeQuery(query);
221
222         while (results.next()
223         {
224             String type = results.getString("cc_type");
225             String num = results.getString("cc_number");
```



Fortify Security Assistant for Eclipse sorts issues based on Fortify Priority Order (Critical, High, Medium, and Low).

- Click the issue to see a detailed description of it in the **Security Help** view.

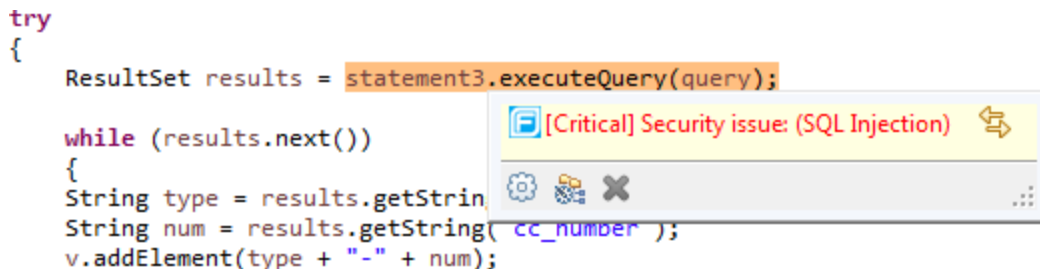


Note: You can page through the visited descriptions in the **Security Help** view with the **Go Back** and **Go Forward**  buttons.



- Select **Fortify > Open Security Issue List** to open the **Security Assistant Issues** view which lists possible issues in the file.
 See "[Working with the Security Assistant Issues View](#)" on the next page for more information.



Working with Issues in the Code

Pause your cursor over the highlighted code to open a tooltip that displays one or more issues. Move your cursor into the Fortify Security Assistant for Eclipse tooltip or press **F2** to access additional options.



The Fortify Security Assistant for Eclipse tooltip displays the icons described in the following table.

Icon	Description
	Specify the categories of issues to show. You can configure settings for the current project or the workspace. Note: Settings configured for a project override the settings for the workspace.
	Configure Fortify Security Assistant for Eclipse annotation preferences.

Icon	Description
	Suppress this issue for the function. This indicates that the issue is not a problem. The issue is not reported again for this function unless you unsuppress it.
	For dataflow issues, go to the origin of the tainted data that reached this function.

Scanning Projects for Issues

You can use Fortify Security Assistant for Eclipse to examine a project and identify any security issues.

To scan a project for issues:

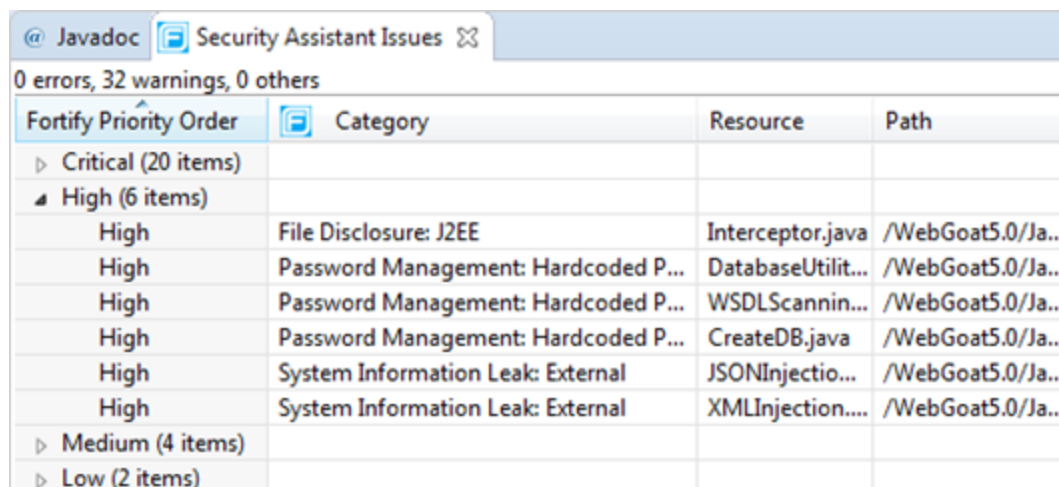
- Right-click the project name, and then select **Inspect the Project**.

Fortify Security Assistant for Eclipse displays any possible issues found in the **Security Assistant Issues** view. For information on how to use this view, see "[Working with the Security Assistant Issues View](#)" below.

Working with the Security Assistant Issues View


The **Security Assistant Issues** view shows all detected security issues for code that has been inspected with Fortify Security Assistant for Eclipse.

Note: These instructions describe a third-party product and might not match the specific, supported version you are using. See your product documentation for the instructions for your version.



Fortify Priority Order	Category	Resource	Path
▶ Critical (20 items)			
▲ High (6 items)			
High	File Disclosure: J2EE	Interceptor.java	/WebGoat5.0/Ja...
High	Password Management: Hardcoded P...	DatabaseUtilit...	/WebGoat5.0/Ja...
High	Password Management: Hardcoded P...	WSDLScannin...	/WebGoat5.0/Ja...
High	Password Management: Hardcoded P...	CreateDB.java	/WebGoat5.0/Ja...
High	System Information Leak: External	JSONinjectio...	/WebGoat5.0/Ja...
High	System Information Leak: External	XMLInjection....	/WebGoat5.0/Ja...
▶ Medium (4 items)			
▶ Low (2 items)			

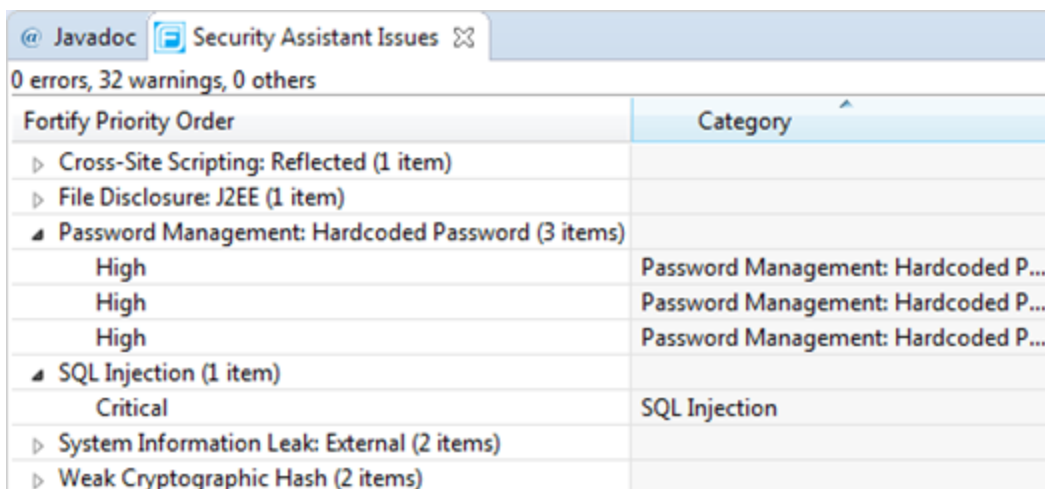
Note: If the **Security Assistant Issues** view is not open, select **Fortify > Open Security Issue List**.

- To see a detailed description of an issue, right-click the issue, and then select **Description**.
The **Security Help** view opens and provides an explanation of the issue, recommendations for fixing the issue, and references related to the issue.
- To go to the location of the issue in the file editor, double-click the issue in the **Security Assistant Issues** view.
- To go to the source location of the tainted data for dataflow issues, right-click the dataflow issue, and then select **Go to Source**.
- To change which issues are shown, click the **View**  menu, select **Show**, and then select one or more of the options listed in the following table.

Option	Description
All Critical Security Issues in Workspace	Shows all critical, non-suppressed issues for Fortify Security Assistant for Eclipse-inspected code in your workspace
All Security Issues in Workspace	Shows all non-suppressed issues for Fortify Security Assistant for Eclipse-inspected code in your workspace
Security Issues on Selection	Shows all non-suppressed issues based on the current selection
All Suppressed Security Issues	Shows all suppressed issues in your workspace
Show All	Shows all issues (including suppressed) for Fortify Security Assistant for Eclipse-inspected code (selecting this option clears the other options in the Show menu) Note: If you clear all of the other show options, the Show All option is automatically selected.

- To change how the issues are grouped, click the **View** menu, select **Group By**, and then select **Fortify Priority Order** (the default view), **Category**, or **None**.

The following example shows issues grouped by **Category**.



Fortify Priority Order	Category
▸ Cross-Site Scripting: Reflected (1 item)	
▸ File Disclosure: J2EE (1 item)	
▲ Password Management: Hardcoded Password (3 items)	
High	Password Management: Hardcoded P...
High	Password Management: Hardcoded P...
High	Password Management: Hardcoded P...
▲ SQL Injection (1 item)	
Critical	SQL Injection
▸ System Information Leak: External (2 items)	
▸ Weak Cryptographic Hash (2 items)	

- By default, the maximum number of issues shown in one group is 100. To change the maximum

number of issues shown, click the **View** menu, select **Filters**, and type a different value in the **Items per group** box.

To display all issues, select **View > Filters**, and then clear the **Use Limits** check box.

- To change the columns that are displayed, click the **View** menu, and then select **Configure Columns**.

Showing Suppressed Issues

Issues that you have suppressed are not highlighted in the source code (even after you restart Eclipse). By default, Fortify Security Assistant for Eclipse does not display suppressed issues in the **Security Assistant Issues** view.



To show the suppressed issues:

- In the **Security Assistant Issues** view, select **View** () > **Show > All Suppressed Security Issues**.

Suppressed issues are indicated in the **Type** column as a **Suppressed Security Issue**.

Unsuppressing Issues

To unsuppress an issue:

1. If the **Security Assistant Issues** view is not open, select **Fortify > Open Security Issue List**.
2. To show the suppressed issues in the **Security Assistant Issues** view, do one of the following:
 - Select **View** () > **Show > All Suppressed Security Issues**.
 - Select **View** () > **Show > Show All**.
3. Right-click the suppressed issue, and then select **Delete**.
4. Right-click the project, and then select **Inspect the Project** to have the issue display in the **Security Assistant Issues** view.

The issue is no longer suppressed.

Hiding Security Issues

You can hide security issues in specified files for the current Eclipse session. Fortify Security Assistant for Eclipse ignores the files during any re-inspection until you either restore (reveal) the security issues for the files or restart Eclipse.

To hide the security issues, do one of the following:

- For a folder, right-click the folder in the Project Explorer or Package Explorer, and then select **Clear Security Issues**.
- For a file, right-click in the file editor, and then select **Clear Security Issues**.

Revealing Previously Hidden Security Issues

You can reveal security issues that you previously hid (cleared) for the current Eclipse session.

To show previously hidden security issues, do one of the following:

- For a folder, right-click the folder, and then select **Restore Cleared Security Issues**.
- For a file, right-click in the file editor, and then select **Restore Cleared Security Issues**.

Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on User Guide (Fortify Security Assistant Plugin for Eclipse 18.20)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to FortifyDocTeam@microfocus.com.

We appreciate your feedback!